SSL/TLS-Entschlüsselung

Veröffentlicht: 2023-09-14

Die Verschlüsselung sensibler Daten ist ein wichtiger Bestandteil des Schutzes Ihrer Netzwerkressourcen. Allerdings verringert die Verschlüsselung auch die Sichtbarkeit des Netzwerk für Cybersicherheit und Forensik. Da verschlüsselter Datenverkehr ein immer häufigerer Vektor für bösartige Aktivitäten ist, empfehlen wir Ihnen, das ExtraHop-System so zu konfigurieren, dass Ihr kritischer SSL/TLS-Verkehr entschlüsselt wird, um Erkennungen zu ermöglichen, mit denen verdächtiges Verhalten und potenzielle Angriffe erkannt werden können.

Die folgenden Anforderungen müssen für die SSL/TLS-Entschlüsselung erfüllt sein:

- Ihr SSL/TLS-Serververkehr muss mit einem verschlüsselt sein unterstützte Verschlüsselungssuite.
- Sie können nur den Datenverkehr für die Dienste entschlüsseln, die Sie in Ihrem Netzwerk bereitstellen und kontrollieren.

Verschlüsselungsarten

Wenn ein Client eine Verbindung zu einem Server über SSL/TLS initiiert, identifiziert eine Reihe von Handshake-Austauschen die Verschlüsselungssuite, die den Satz von Algorithmen enthält, der die Daten verschlüsselt und die Datenintegrität authentifiziert.

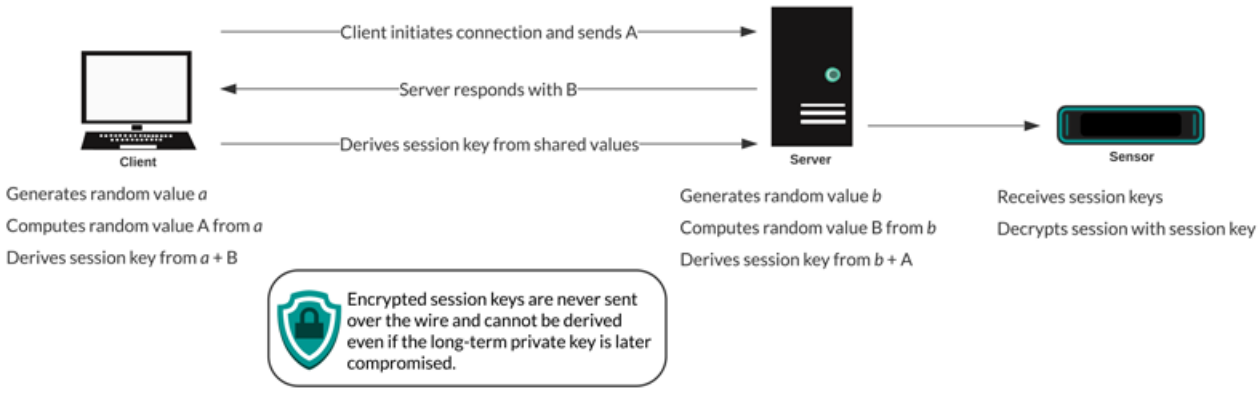
Sie können das ExtraHop-System so konfigurieren, dass der SSL/TLS-Verkehr auf der Grundlage des Typs entschlüsselt wird unterstützte Verschlüsselungssuite mit dem die Netzwerkverbindung gesichert ist.

Video: Erfahren Sie mehr über Verschlüsselung.

Weiterleitung von Sitzungsschlüsseln

Wenn die Weiterleitung von Sitzungsschlüsseln auf dem ExtraHop-System aktiviert ist, kann ein schlanker Agent auf dem Server installiert werden, der Sitzungsschlüssel an das System weiterleitet, und das System kann den zugehörigen SSL/TLS-Verkehr entschlüsseln. Die Kommunikation zwischen dem Key Forwarder und dem System ist mit TLS 1.2 verschlüsselt.

Perfect Forward Secrecy (PFS) Cipher Suites leiten gegenseitig einen Sitzungsschlüssel durch eine Reihe von Austauschen zwischen dem Client und dem Server ab. Nur der Client und der Server kennen den Sitzungsschlüssel, der niemals über das Drahtnetz gesendet wird. Selbst wenn der langfristige Serverschlüssel kompromittiert wird, bleibt der kurzlebige Sitzungsschlüssel sicher.



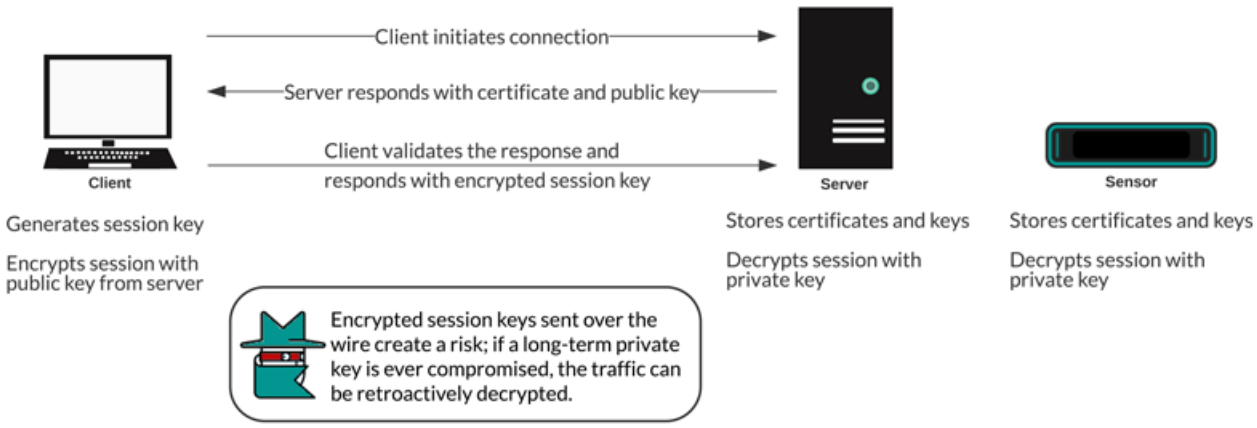
Zertifikate und Schlüssel

Wenn ein Zertifikat und ein privater Schlüssel für unterstützte Cipher Suites werden auf ein ExtraHop-System hochgeladen, das System ist in der Lage, den zugehörigen SSL/TLS-Verkehr zu entschlüsseln.

Hinweis: TLS 1.2 und früher unterstützen RSA für den Schlüsselaustausch, TLS 1.3 jedoch nicht.

Cipher Suites für RSA können mit einem Serverzertifikat und einem privaten Schlüssel entschlüsselt werden. Wenn ein Client über SSL/TLS eine Verbindung zu einem Server herstellt, antwortet der Server mit einem Zertifikat, das seine Identität bestätigt und den öffentlichen Schlüssel teilt. Der Client generiert und verschlüsselt einen Sitzungsschlüssel und sendet den verschlüsselten Sitzungsschlüssel an den Server. Der Client überprüft, ob das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle signiert wurde und ob der Server mit der angeforderten Domäne übereinstimmt.

Da der verschlüsselte Sitzungsschlüssel während des Handschlag über das Drahtnetz gesendet wird und der private Schlüssel langfristig auf dem Server gespeichert wird, kann jeder, der Zugriff auf den Datenverkehr, das Serverzertifikat und den privaten Schlüssel hat, den Sitzungsschlüssel ableiten und die Daten entschlüsseln. Teams, die für die Verschlüsselung ihres Datenverkehrs verantwortlich sind, zögern möglicherweise, private Schlüssel mit anderen Geräten im Netzwerk zu teilen, um das Risiko zu minimieren.



Bewährte Verfahren

Hier sind einige bewährte Methoden, die Sie bei der Implementierung der SSL/TLS-Verschlüsselung berücksichtigen sollten.

- Schalten Sie SSLv2 aus, um Sicherheitsprobleme auf Protokollebene zu reduzieren.
- Schalten Sie SSLv3 aus, sofern es nicht aus Gründen der Kompatibilität mit älteren Clients erforderlich ist.
- Schalten Sie die SSL-Komprimierung aus, um die CRIME-Sicherheitslücke zu vermeiden.
- Schalten Sie Sitzungstickets aus, sofern Sie nicht mit den Risiken vertraut sind, die PFS schwächen könnten.
- Konfigurieren Sie den Server so, dass er die Verschlüsselungssuite in der Reihenfolge der Serverpräferenz auswählt.
- Beachten Sie, dass die Weiterleitung von Sitzungsschlüsseln die einzige Option für mit TLS 1.3 verschlüsselten Datenverkehr ist.

Welcher Verkehr soll entschlüsselt werden

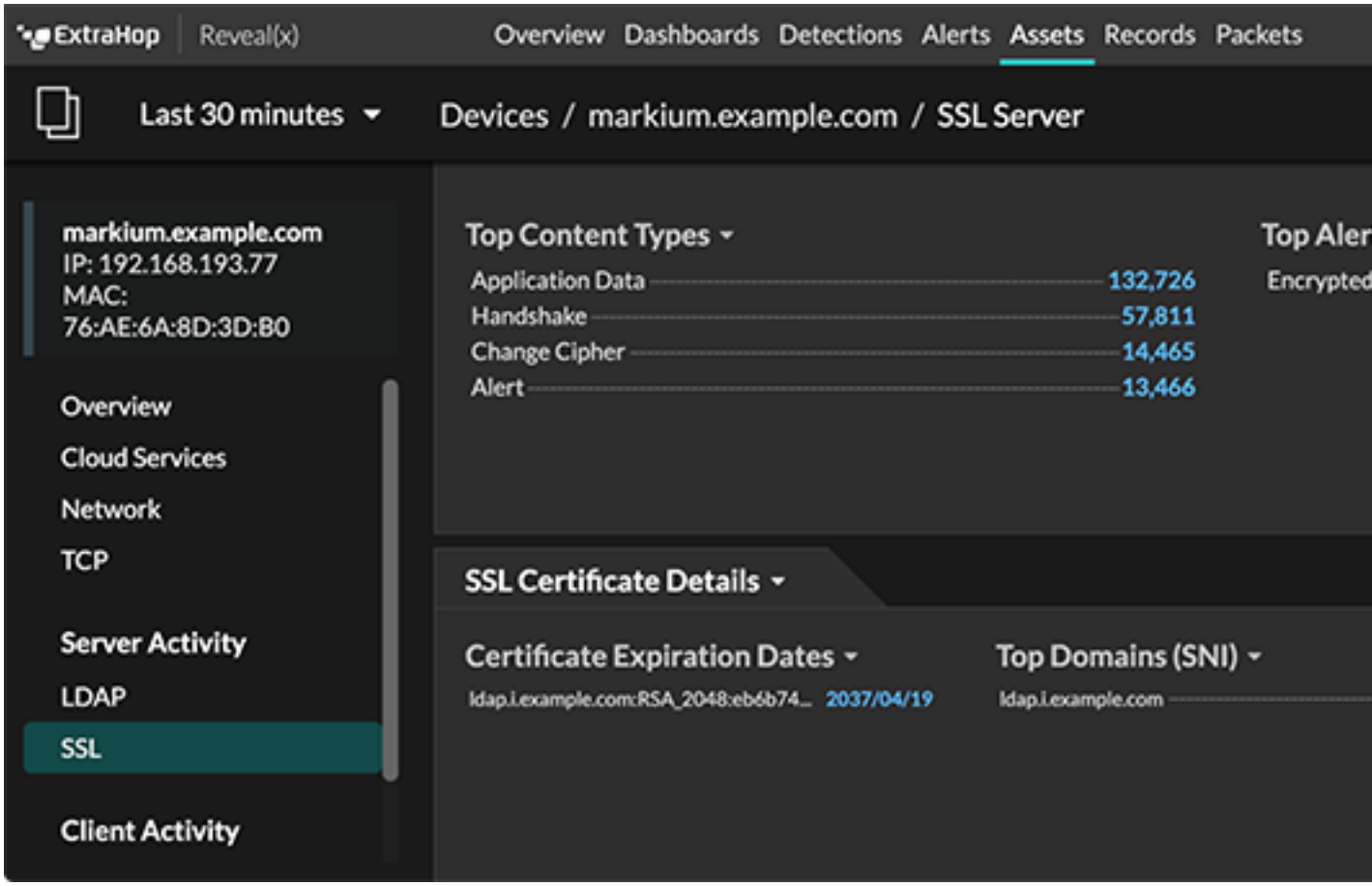
Der Datenverkehr, den Sie untersuchen möchten, enthält wahrscheinlich vertrauliche Daten, sodass das ExtraHop-System keine entschlüsselten Nutzdaten auf die Festplatte schreibt. Das ExtraHop-System analysiert den Datenverkehr in Echtzeit und verwirft dann den Sitzungsschlüssel, sofern keine Trace-Appliance für die kontinuierliche PCAP eingesetzt wird. Optional kann das System so konfiguriert werden, dass der Sitzungsschlüssel zusammen mit den Paketen gespeichert wird. Dies ist sicherer, als den langfristigen privaten Schlüssel mit Analysten zu teilen.

Hier sind einige Beispiele für die Art von Daten, die Sie in Betracht ziehen sollten, mit dem ExtraHop-System zu entschlüsseln:

- Die Entschlüsselung von sicherem HTTP (HTTPS) -Verkehr, der zwischen einem Server und einem Client über eine SSL/TLS-Verbindung ausgetauscht wird, kann zu Angriffen auf Webanwendung wie SQL Injection (SQLi) und Cross-Site Scripting (XSS) führen, die zu den häufigsten Sicherheitsrisiken für Webanwendung auf der Die 10 besten OWASP Liste. Durch die Entschlüsselung von HTTPS-Verkehr können auch Exploit-Mechanismen aufgedeckt werden, z. B. ein bösartiger URI oder ein Abfrageparameter, für häufig auftretende Sicherheitslücken und Exposures (CVEs) in Webanwendungen und Servern.
- Die Entschlüsselung von sicherem LDAP-Verkehr (LDAPS), der zwischen einem LDAP-Server und einem Client über eine SSL/TLS-Verbindung ausgetauscht wird, kann Aufklärungsaktivitäten nach sich ziehen. Das BloodHound-Angriffstool verschlüsselt beispielsweise LDAP-Abfragen mit SSL/TLS (sowie Kerberos oder NTLM), um große Listen von Active Directory-Objekten zur Erkundung zu sammeln. Durch die Entschlüsselung des LDAPS-Verkehrs kann auch der Exploit-Mechanismus für den kritischen CVE aufgedeckt werden, der als Log4Shell.
- Bei der Entschlüsselung von MySQL-, PostgreSQL-, MS SQL Server- oder Oracle-Datenbankverkehr, der zwischen einem Datenbankserver und einem Client über eine SSL/TLS-Verbindung ausgetauscht wird, können bösartige Anweisungen oder Befehle auftauchen, die darauf abzielen, Daten zu löschen, zu ändern oder zu lesen.
- Durch die Entschlüsselung von Datenverkehr, den Sie möglicherweise für forensische Prüfungen benötigen, können Sie Compliance-Vorschriften einhalten oder Vorfälle auf kritischen Systemen untersuchen, z. B. in Ihren Kundendatenbanken, Systemen, in denen wertvolles geistiges Eigentum gespeichert ist, oder auf Servern, die wichtige Netzwerkdienste bereitstellen.

Sie können auch die Art des verschlüsselten Datenverkehrs für ein bestimmtes Gerät identifizieren, das vom ExtraHop-System erkannt wurde. Finde das Gerät im System und navigieren Sie zur Gerätedetailseite.

Klicken Sie im linken Bereich auf **SSL** im Abschnitt Serveraktivität. Scrollen Sie im mittleren Bereich zum Diagramm Top Cipher Suites.



So entschlüsseln Sie Ihren SSL-Verkehr

Wie Sie SSL-Verkehr entschlüsseln, hängt von der Verschlüsselungssuite und Ihrer Serverimplementierung ab.

Hinweis: siehe unterstützte Cipher Suites um zu erfahren , welche Cipher Suites entschlüsselt werden können und welche Anforderungen sie haben.

Wenn Ihr SSL-Verkehr mit PFS-Cipher Suites verschlüsselt ist, können Sie die ExtraHop Session Key Forwarder-Software auf jedem Server installieren, auf dem der SSL-Verkehr gespeichert ist, den Sie entschlüsseln möchten. Der Sitzungsschlüssel wird an das ExtraHop-System weitergeleitet und der Verkehr kann entschlüsselt werden. Beachten Sie, dass Ihre Server die Session Key Forwarder-Software unterstützen müssen.

- Installieren Sie den ExtraHop Session Key Forwarder auf einem Windows-Server
- Installieren Sie den ExtraHop Session Key Forwarder auf einem Linux-Server

Wenn Sie über einen F5-Load Balancer verfügen, können Sie Sitzungsschlüssel über den Balancer gemeinsam nutzen und vermeiden, die Software zur Weiterleitung von Sitzungsschlüsseln auf jedem Server zu installieren.

- Weiterleitung von Sitzungsschlüsseln von einem F5-LTM

Wenn Ihr SSL-Verkehr mit RSA Cipher Suites verschlüsselt ist, können Sie trotzdem Session Key Forwarder-Software auf Ihren Servern installieren (empfohlen). Alternativ können Sie das Zertifikat und den privaten Schlüssel in das ExtraHop-System hochladen.

- Entschlüsseln Sie den SSL-Verkehr mit Zertifikaten und privaten Schlüsseln

Wir empfehlen, dass Sie nur den Verkehr entschlüsseln, den Sie benötigen. Sie können das ExtraHop-System so konfigurieren, dass es nur bestimmte Protokolle entschlüsselt und Protokollverkehr nicht standardmäßigen Ports zuordnet.

- Verschlüsselte Protokolle hinzufügen
- Fügen Sie einen globalen Port zur Protokollzuordnung hinzu

Pakete für forensische Audits entschlüsseln

Wenn Sie eine Trace-Appliance oder einen anderen Packetstore konfiguriert haben, können Sie Sitzungsschlüssel auf der Trace-Appliance speichern und Sitzungsschlüssel mit Paketerfassungen herunterladen, sodass Sie die Pakete in einem Paketanalyse-Tool wie Wireshark entschlüsseln können. Mit diesen Optionen können Sie den Datenverkehr sicher entschlüsseln, ohne langfristige private Schlüssel mit Analysten teilen zu müssen.

Das System speichert nur Sitzungsschlüssel für Pakete auf der Festplatte. Wenn Pakete überschrieben werden, werden die zugehörigen gespeicherten Sitzungsschlüssel gelöscht. Nur Sitzungsschlüssel für entschlüsselten Datenverkehr werden zur Speicherung an die Trace-Appliance gesendet. Das ExtraHop-System sendet den Sitzungsschlüssel mit den zugehörigen Flussinformationen an die Trace-Appliance. Wenn ein Benutzer über Pakete und Sitzungsschlüsselrechte verfügt, wird der Sitzungsschlüssel bereitgestellt, wenn im abgefragten Zeitraum ein entsprechender Fluss vorhanden ist. Überflüssige Sitzungsschlüssel werden nicht gespeichert, und die Anzahl der Sitzungsschlüssel, die das ExtraHop-System empfangen kann, ist unbegrenzt.

Wir empfehlen, Vorsicht walten zu lassen, wenn Sie ExtraHop-Systembenutzern Rechte gewähren. Sie können die Privilegien angeben die es Benutzern ermöglichen, Pakete anzusehen und herunterzuladen oder Pakete und gespeicherte Sitzungsschlüssel anzusehen und herunterzuladen. Gespeicherte Sitzungsschlüssel sollten nur Benutzern zur Verfügung stehen, die Zugriff auf vertraulichen, entschlüsselten Datenverkehr haben sollten. Das ExtraHop-System schreibt zwar keine entschlüsselten Nutzdaten auf die Festplatte, aber der Zugriff auf Sitzungsschlüssel ermöglicht die Entschlüsselung des zugehörigen Datenverkehrs. Um eine durchgängige Sicherheit zu gewährleisten, werden die Sitzungsschlüssel beim Wechsel zwischen Geräten sowie bei der Speicherung der Schlüssel auf der Festplatte verschlüsselt.

- Speichern Sie SSL-Sitzungsschlüssel auf verbundenen Trace-Appliances
- Laden Sie Sitzungsschlüssel mit Paketerfassungen herunter